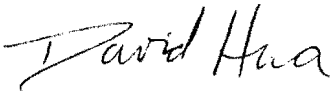
Making the Case for Ethical Hacking

An Honors Thesis (HONRS 499)

by

Michael Wulff

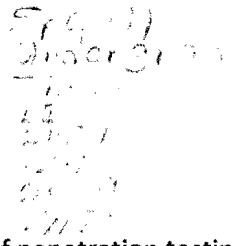
Thesis Advisor
David Hua



Ball State University
Muncie, Indiana

June 2009

July 25, 2009



Abstract

The objective of penetration testing is to attack computer networks, without causing harm, in order to find the security gaps present. The financial impacts of being hacked are discussed and explored. Penetration testing is a proactive and highly valuable mean of securing information on computer networks. Both government and industry regulations find penetration testing to be a necessary part of yearly security audits. A number of certifications have been developed to identify those with the necessary skills to conduct penetration tests. This paper helps build a business model for ethical hacking teams. This model is done through the discussion and evaluation of testing methods, team resources, and the handling of a hypothetical client.

Acknowledgements

-I wish to thank Professor David Hua for advising me through this project. He was extremely helpful in helping me develop my paper and helping me with my revisions.

-I would like to also thank Kellie Patton for her volunteering to help me edit my paper.

Introduction

The world today is becoming more and more technology dependent. The security of personal information in today's world relies on far more than simply a locked door. Security today relies heavily on safe guards, procedures, and policies that are put into place and left to be. But are those measures enough to offer real security? Without testing the security measures in place to prove they work, is it really security, or just a false sense thereof? The only way to know a computer is safe from hackers is to try and have it hacked. The purpose of this thesis paper is to explore, explain, and evaluate the importance of ethical hacking to our business world. Further, I set out to build a basic business model for a hypothetical hacking team.

The Impact

Before I begin explaining my rationale for building a team it is best to start off explaining what "hacking" is and where the term comes from. The word "hacking" comes from the word hack, which Webster's Dictionary (2009) defines as, "to gain access to a computer illegally." The word often used to describe someone who breaks into computers; the illegality of the action is often implied. There are two words that actually refer to people who break into computer systems, hackers and crackers. In the early 90's the term hacker was used to define someone who could access systems. The term cracker was used to distinguish someone who would access systems to damage them. Eventually the term hacker came to cover both terms.

People hack systems for a wide variety of reasons, some of which are better than others. These reasons can be covered with two blanket ideas. The first thought would

be in line with Dana Hinders's (2009) view that hackers are people who often enjoy programming and applying what they know to demonstrate their abilities and technical skills, not to cause harm unto others. The other group is "out to steal personal information, change a corporation's financial data, break security codes to gain unauthorized network access, or conduct other destructive activities are sometimes called 'crackers'" (Hinders, 2009). These two views broadly cover the reasons why people will attempt to access computer systems without authorization.

The impact of computer hacking is incredible. It not only creates a financial impact to organizations and individuals, but it also has a social impact. The financial damages associated with hacking have sky rocketed since 1995 the Senate's Permanent Investigations Subcommittee (Ricciuti, 1996) estimated the damages of hacking to be $800 million. The global financial impact of hacking is estimated to be roughly $1 to1.6 trillion dollars in 2008, a substantial jump from 1995 (Mills, 2009). On a smaller scale the average cost of a private information leak in 2007 averaged at $6.3 million dollars, which is a $1.5 million dollar increase from the year previous (Greenburg, 2007). When financial organizations or even federal organizations have private records stolen, hacked, it incurs a cost per record. Security firms Vontu and PGP concluded that it cost, on average, $198 for each personal record breached or lost (Greenburg, 2007). In 2005 VISA and MasterCard together had over 40 million card accounts exposed to fraud due to a security breach (Sahadi, 2005). However, only 200,000 accounts were fully exposed which has an estimated financial cost of $39.6 million dollars; whereas the damage incurred by the forty million accounts would have been roughly $7.92 billion.

The impact of being hacked goes far beyond the simple financial damage. Getting hacked can also deteriorate a business's reputation, especially if it hinges on protecting clients' personal information. The impact goes further than that though. When the mere report of a security breach occurs, customers leave the companies and the impact to the company's stock can be devastating. To further illustrate the impact of being hacked, the company responsible for the forty million exposed credit cards, CardSystems, lost valuable business with large credit card companies such as VISA and MasterCard (Freed, 2009).

With private personal information accessible to those with mal intent, the impact extends beyond the company itself and onto their now former clients. The security risk I am referring to is identity theft. The Federal Trade Commission refers to identity theft as the instance when, "someone uses your personally identifying information, like your name, Social Security number, or credit card number, without your permission, to commit fraud or other crimes" (2009). According to a Javelin Strategy and Research (2007), roughly 8.4 million Americans were victims of identity theft, causing roughly $50 billion dollars in damages.

If hacking is so dangerous, what can be done to prevent it? To protect against computer hackers, there are few simple things that can be done, such as using a strong password, using a fully updated operating system, using anti-virus and using a firewall (ITEDU 490, 2009, pg. 41). Yet, how does one know these fortifications will hold up against an attack? The simple answer is, "You don't." There is simply no way to be sure your system is completely secure from attacks until it is actually attacked. For, as Orson Scott Card puts it, "There is no teacher like the enemy...Only the enemy shows

you where you are weak" (2002, pages 262-263). This quote forms the foundation of a concept called penetration testing (ethical hacking), a valuable tool used by governments and businesses alike.

Ethical Hacking

The concept has been introduced, but just what is ethical hacking? Kevin Beaver defines ethical hacking as good guys who "hack a system to discover vulnerabilities for the purpose of protecting computers against illicit entry, abuse, and misuse" (2004, page 10). The purpose of doing this is to find better ways of securing the holes present in system security. As mentioned before, there is simply no way to adequately secure your system without having it tested; it is much akin to perfecting an essay without ever having it proofread.

Ethical hacking, also known as a penetration testing, offers a range of benefits to an organization. In an interview with Network Computer, security specialist Chris O'Ferrell (2001) described the biggest benefit from conducting a penetration test as retaining "customer trust." Customers want to know that something is safe and secure and seek out businesses and organizations like that. O'Ferrell drives the point home when he asks what would happen if a customer logs into their online banking system and sees the bank's homepage maliciously changed by a hacker. The answer he gives is that one loses the customer's trust, and more importantly, their business. O'Ferrell and his colleague Ira Winkler stress heavily that penetration testing is a preventative measure that "alerts businesses to their vulnerabilities before the hackers have a chance to exploit them" (2001).

The cost of a penetration test runs anywhere from $5,000 to $50,000 or more depending on depth of the test and the individual or team conducting it (PLYNT, 2006). With data breaches costing organizations $613,000 to $32,000,000 on average, it makes financial sense to conduct penetration testing (Mills, 2009). It should be noted that these figures do not fully account for the loss of current customers or more importantly future customers lost due to the breach in security.

While penetration tests offer the benefit of allowing you to tighten your security there are some risks associated with performing them. Winkler and O'Ferrell (2001) both feel that there is a risk of gaining a false sense of security; either because of a poorly performed penetration test or because penetration tests never find all vulnerabilities. If the penetration test fails to uncover a bad security practice, it will often go unchecked and continue to be a danger to system security. One of the more worrying questions is, if something goes wrong, who is responsible for the damages and what plans are in place to repair them? This is defined well before the penetration test is even conducted and is overseen by both information technology (IT) staff and lawyers.

Conducting a Penetration Test

Penetration tests can be conducted in two manners. The first is announced, where the system administrators are actively involved and closing the holes, security gaps, as they are discovered, and unannounced, where the system administrators are completely unaware a test is being conducted. According to the authors of *Hack I.T.*, the problem with announced penetration tests is that administrators are closing the security holes as they are notified of them (Klevinsky, Laliberte, & Gupta, 2002, pg 27). This means that these security holes cannot be fully explored and evaluated; which leaves

the extent of the vulnerability relatively unknown as some small holes lead to major ones if discovered and exploited. The impact of such an oversight can be extremely damaging and costly. Unannounced tests can go just as badly if management is unaware of IT's schedule. For instance, they may mistakenly schedule a penetration test the same day when a system administrator is performing system and network maintenance. This occurrence means services could be disabled or servers shutdown; which will skew the results of the penetration test, making it not nearly as useful or accurate.

Announced penetration tests have few consequences apart from vulnerabilities being shutdown as they are noted, leaving the administrator unaware of how damaging or deep that hole might have been. The authors of *Hack I.T.* presented hubris as one of the associated risks of an announced penetration test (Klevinsky et al, 2002, pg. 27). This risk is based on the concept that the IT administrator would like to present their system as very secure and changes the security settings prior to the test to make it substantially more secure. The problem is that if the settings are reverted after the penetration test is conducted, unknown vulnerabilities are still present and ones that had been corrected in the stronger settings may no longer apply.

One of the more worrying ways in which an unannounced penetration test can go wrong is:

> *The risk with unannounced testing is that since the security administrators do not know that a test is being performed, they will respond as they would to a hacker and block the penetration testing efforts (drop connections, reboot machines, and so on). This would indicate a good*

> *response/detection process is in place, but it can cut a test short. The [real] danger with this test is that occasionally security administrators have been known to contact the relevant authorities to report the penetration activities (*Klevinsky et al, 2002, pg. 27*).*

Clearly there is a market segment that has uses and needs penetration testing. While the concept, necessity, and benefits of penetration testing have been discussed, the manner of how a penetration test is conducted has not yet been examined.

Methods of Approach

Penetration tests can, as previously discussed, be announced or unannounced in nature. The tests themselves, depending how thorough an organization wishes them to be, are often composed of 3 distinct parts. The three parts of an average penetration test are external testing, internal testing, and social engineering (Mullins, 2005). These parts of a penetration test can either be performed separately or all at the same time. Depending on the size of the team and the resources available, performing a penetration test focusing on all three areas at once obviously puts a much greater strain on the testing organization than performing each phase separately.

External Penetration Testing

As previously mentioned, penetration testing takes place on three different levels or areas: the external, the internal, and on the social level. The most recognizable and understandable of these three is the external penetration test. This test can be conducted in one of two ways. Either the attacker can have knowledge of what all the external systems are or they have to research what systems are connected externally through research and publicly available data. The external penetration test is used to

test the outer walls of a business's computer network. This means services that are publicly accessible from the internet such as Web Servers, E-mail, DNS server (Domain Name System), and even firewalls are tested for vulnerabilities (Mehta, 2005). The purpose of the external test is to get past external systems and gain access to other vital internal systems. Even if a penetration test cannot breach the external systems to gain access to the internal network, being able to exploit the external systems, such as web servers, can have devastating results. Allen Stern (2008) describes the impact this could have to an organization by calculating how much it would cost Amazon.com for each minute the site was inaccessible, which amounts to approximately $31,000 each minute.

Internal Penetration Testing

There is simply no way to completely secure a computer from any sort of attack; meaning it is merely a matter of time before a system is compromised. As the goal of an external penetration test is to find the vulnerability in a system that allows the infiltrator access to the internal network, it becomes vital to find the weaknesses in regard to internal network security in order to protect integral internal systems. Puneet Mehta (2008) describes internal penetration tests as tests that are performed within an organization's technology environment. He says the purpose of these tests is to "mimic an attack on the internal network by a disgruntled employee or an authorized visitor having standard access privileges" (2008). These kinds of tests will allow an organization to fully understand how vulnerable their systems are should their network perimeter be successfully penetrated.

The primary concern of an internal penetration test is not necessarily to test what the internal system vulnerabilities and exploits are, though this part is definitely a serious aspect, but rather to see if "it possible for someone connected to the internal network to gain access to areas of your network that he is not privileged" (eHosting Datafort, 2004) to access. This occurrence usually takes the form of an internal user having low level access or even a trusted user who abuses their trusted status to obtain access to private areas of a network.

Social Engineering

Social engineering is quite possibly the most seemingly out of place method of testing the security of a computer network. Internal and external penetration testing methods rely heavily on technical knowhow and sophisticated security programs whereas social engineering works on exploiting vulnerabilities in people to gain access to otherwise unauthorized information or materials (Mullins, 2005). Common examples of social engineering seem innocent in nature such as reading over someone's shoulder, looking at their sticky notes for passwords, dumpster diving, or even faking a sales call to an IT department claiming to sell a new firewall only to be told that they are already using a specific firewall.

Social engineering tends to be a controversial inclusion to a penetration test. As previously mentioned social engineering is considered by some to not be truly part of the penetration testing because it is not technical in nature. Ed Skoudis (2008) makes the point that "security personnel need to cultivate deep trust with all employees in their enterprise. Without this trust, these employees may ignore the security advice from people who have duped them in the past as part of a social engineering exercise during

a penetration test." While this mishap is the major argument against using social engineering, it is easily diffused by not naming employees guilty of divulging information. By doing so, trust is retained and all members of the organization benefit from the experience.

Information can be gathered by using social engineering in an attempt to use people to circumvent security systems. The size of an organization often correlates to how effective social engineering attempts can be if adequate security procedures are not in place. As an organization grows, it becomes more susceptible to social engineering techniques. This problem is due to the lack of face-to-face interaction with fellow employees in larger organizations. Members with smaller businesses often have greater face-to-face interaction with fellow employees. This interaction makes it harder for outside people to pose as employees or circumvent security procedures as fellow employees have closer working relationships.

The benefit of social engineering is that it helps organizations "evaluate the efficacy of security awareness training or test employee adherence to standards of conduct. It can help to reveal poor security practices, policy gaps or low security vigilance" (Priester, 2008). Dumpster diving for information, for example, can reveal if an organization is properly disposing of its sensitive information. If someone is trying to access information or resources not available to them and are gaining access, it will let employers know if procedures are being properly followed. A less invasive method is to interview employees about security procedures and present them with test situations to see how they would handle them.

By using social engineering in a penetration test, organizations are rewarded with evidence as to whether or not their current security measures to safe guard critical and sensitive information are working. Specific findings can help an organization design and implement better awareness and training in a quick and cost effective manner. As part of a penetration test, social engineering is helpful in finding more ways to better protect an organization's information that cannot be done through traditional computer security.

Regulations and Certifications

FISMA

The Federal Information Systems Management Act (FISMA) enacted in 2002 "requires each federal agency to develop, document, and implement an agency-wide program to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source" (NIST, 2009). Essentially any organization that works with the Federal government must provide information security to those systems. This would be rather unremarkable was it not for NIST SP 800-53A, as broken down by Core Security Technologies:

> *With this requirement, NIST has recommended that all such organizations proactively test their network and IT defense mechanisms using assessment techniques that simulate the actions of real-world attacks. The details of NIST Special Publication 800-53A specifically demand penetration testing that goes beyond the use of scanners to exploit vulnerabilities and demonstrate how security controls have been tested*

against the same types of multi-staged attacks that are being aimed at their assets on a daily basis (2009).

HIPAA

In 1996 Congress enacted Health Insurance Portability and Accountability Act (HIPAA) as a means of healthcare reform. HIPAA's goal is to provide a national standard for electronic health care transactions and to protect health insurance coverage in the midst of job transition or job loss. HIPAA further provides for a series of security baselines necessary to protect citizens' medical information. Penalties for non-compliance can reach $25,000 per violation a year, and a wrongful disclosure can include fines of up to $250,000 and up to ten years imprisonment ($CORE_1$, 2009). An annual penetration test from a third party is required as part of the criteria to be in compliance.

PCI DSS

Payment Card Industry Data Security Standard (PCI DSS) is a worldwide information security standard that was created to help organizations that process card payments prevent credit card fraud. The reduction in frauds was to be through increased controls around how the data is stored and restricted (PCI Security Standards Council, 2009). Originally, Visa, MasterCard, American Express, Discover, and JCB had their own security standards in place to form a baseline of security that merchants were to meet to ensure customer data (Koonammavu, 2008). According to PCI DSS guidelines, a penetration test is to be performed at least once a year and following any major network changes (PCI DSS Guru, 2008). The organization performing the annual penetration test needs to develop a test that fulfills these two guidelines:

- Evaluate both the network and application layers
- Include both internal and external testing

Sarbanes-Oxley

Sarbanes-Oxley (SOX) was a congressional reaction to the gross corporate financial scandals such as Enron and WorldCom. The goal of SOX is to protect investors by improving the accuracy and reliability of corporate disclosures made pursuant to the securities laws (SOX-Online, 2006). The range of such legislation applies to all companies listed on the New York Stock Exchange. One of the many of standards needed to meet SOX compliance is to conduct a penetration test at least once a year.

Certifications

Federal regulations and industry standards mandate or "strongly" encourage penetration testing to ensure information systems security. It is no surprise that these regulations and "recommendations" also require certain certifications to be obtained by the penetration testing unit. Department of Defense Directive 8570 stated that any "full- or part-time military service member, contractor, or local nationals with privileged access to a DoD information system performing information assurance (security) functions... are required to carry an approved certification for their particular job classification. (SANS, 2009)" This directive makes it a requirement for those in and associated the Department of Defense who have IT security responsibilities to become certified. While there are currently no regulations that state those conducting penetration tests must be certified, it is an expectation of both clients and employers.

Currently there are a wide range of security based certifications for those looking to be certified in or skills necessary for penetration testing. While there are dozens of certifications, a handful are continually referenced and are considered to be not only "worth it" by the computer security industry, but by the community as well.

GPEN

GPEN is a recently developed GIAC Certified Penetration Tester certification. This course was developed Ed Skoudis, a well established IT security professional, to cover network penetration testing and ethical hacking. The certification focuses not only on hands-on experience with the technical tools necessary for penetration testing and vulnerability assessments, but also how to develop an effective penetration test structure and to establish rules of operation with a client organization (EthicalHacker, 2009). The certification strongly focuses on the use of penetration testing tools and how they work together. One of the greatest benefits is the goal of the certification to help develop problem solving skills necessary to surmount obvious difficulties that arise in penetration testing and how they fit into a comprehensive enterprise information security program.

OSCP

The Offensive Security Certified Professional certification is a certification designed for network administrators and security professional that need to become familiar with the world of offensive security. While the certification is considered to be something of a professional level introductory course it goes beyond simply instructing how to use penetration testing tools and actually explains the processes and reasoning behind them. As the course is designed for system administrators, the goal is to make

sure that true skills are developed so that they can be applied in the recipient's parent organization (Offensive-Security, 2009).

CISSP

The Certified Information Systems Security Professional (CISSP) is an independent information security certification governed by the International Information Systems Security Certification Consortium also known as (ISC)² (CramSession, 2009). The certification is formally approved by the U.S. Department of Defense in both their Information Assurance Technical and Managerial categories (Department of Defense, 2008). Further, the CISSP is adopted as the baseline for the U.S. National Security Agency's ISSEP program, which is a study concentration after completion of the CISSP.

The CISSP certification is an advanced certification meant for IT security professionals. Requirements for the certification are five years of full-time security work experience in two or more of the ten ISC^2 Information Security domains, which range from access controls to telecommunications and network security. Both a bachelor's degree and a master's can substitute for time towards the experience requirement.

CISSP certification's goal is to build security professionals. One of the ways it sets out to achieve this is through the recertification process, which takes place every three years. The renewing of the certification becomes part of the belief in continued learning. In order to renew a CISSP certification the credential holder must complete 120 Continued Profession Education credits (CPEs) (CramSession, 2009). CPEs can be earned for a wide variety of activities such as completing new certifications, writing articles, volunteering, attending conferences, teaching, etc in the following ten ISC^2 Information Security domains:

- Access Control
- Application Security
- Business Continuity and Disaster Recovery Planning
- Cryptography
- Information Security and Risk Management
- Legal, Regulations, Compliance and Investigations
- Operations Security
- Physical (Environmental) Security
- Security Architecture and Design
- Telecommunications and Network Security (ISC2, 2009)

The CISSP certification sets an impressive standard for what is expected of the holder. However the CISSP is not the "best" certification nor are the others that are presented. The CISSP views itself as a part of continual learning so that security professionals are able to expertly secure their computer networks.

Penetration Testing Resources

Penetration testing teams need three basic but critical resources in order to complete their projects. Hardware platform, penetration testing tools (software), and personnel make up the three different resources necessary for conducting a penetration test.

Penetration Testing Tools

Penetration testing tools are obviously vital to the success of a penetration test. Penetration testing tools, also known as vulnerability scanners, are programs made for the purpose of searching out computer networks and mapping the weaknesses in an application, computer, or network (Bradley, 2004). A wide variety of information can be retrieved from a scan such as Internet Protocol (IP) addresses, open ports, operating systems, running applications, and even how recently patched the operating system or

applications are. There are vulnerability scanners that can go beyond merely searching for vulnerabilities and actually progress to exploiting them. Scanners such as that can be used in penetration testing, but the goal is to test the network's security, not to bring it to a crashing halt.

There is an extensive range of penetration testing tools available on the market. Some of the tools available are open source software (OSS) and others are proprietary software. There are a myriad of benefits and consequences associated with each type. The easiest difference to be noticed upfront is cost. While professional level proprietary penetration testing tools can cost tens of thousands of dollars, OSS tools cost nothing (Tayal, 2009).

OSS tools have a number of benefits apart from affordability. One of the major benefits associated with OSS tools are their flexibility. As users are able to access the source code to OSS, it allows in-house coders to customize the software to their particular needs. OSS is often community enhanced by the release of personal patches that add additional functionality or patch a flaw in the code that has not yet been fixed in the current version.

If a penetration team does not have in-house programmers to help enhance the OSS, the feature rich proprietary software presents itself as a worthy addition to the team. While proprietary software offers a far greater selection of features, it ends up consuming far larger amounts of memory and CPU power, even if only a few select features are needed. OSS traditionally runs lighter, offering fewer features in each application, but these features are chosen by community need.

The major advantage of choosing proprietary software is the software support offered by the developer (CORE, 2009). When a company sells a piece of its software, it stands proudly behind it assuring that it will work as intended and if it does not, the company will assist. OSS offers little assurance that software will work as intended or that it will be supported long term (Tayal, 2009). OSS is community driven and will be only supported as strongly as the community behind it. Proprietary software developers even offer professional training with their software to make sure the most use can be garnered with it. While some OSS does have professional level training, not all of it does and therefore relies on a community to support it.

The choice between proprietary software and OSS is a difficult one often to make. The best solution is usually to choose the appropriate proprietary software package for the team's needs and to augment this with OSS. Doing so establishes a solid base of reliable and critical features while still being able to use OSS to extend the range and flexibility of the team.

Personnel

Software is an important part of a penetration test, but not nearly as important as the people behind the software, the penetration testers themselves. It is often said that a computer is only as good as the person who uses it. This expression shows how critical it is to hire and develop quality penetration testers.

There are often a wide variety of criteria that needs to be met to get a career in the world today, and penetration testing is no different. While there are a great number of different things organizations do look for, three stand out above the rest: passion for what they do, good communications skills, and if they are competent (Chandran, 2008).

Businesses in today's world look for good communication skills. Roshen Chandran (2008) specifically mentions the ability to correctly and fluently speak English as one of the criteria for PLYNT, a penetration testing firm. As findings in the tests are given to the client in the form of a report it makes sense that communication skills are required. As the goal of such a test is to improve the client's security being able to clearly explain the security problem and its solution, even to non-technical people, is simply part of the job.

It was surprising to see competency as of one of the many qualities in consensus, though it does make perfect sense. The IT field is filled with people who possess certifications that can be easily studied for and earned without any form of a practical testing them on that knowledge (Security Monkey, 2006). Certifications with a practical demonstrate competency with the skills and knowledge set by the certification. Further, being able to analytically approach a problem is helpful as there are penetration testing methodologies that rely on this.

Being passionate about what you do is a quality that will take someone far in IT. As IT is a constantly evolving field, new things are to be learned on a daily basis. It takes a lot of effort to stay current on the latest system vulnerabilities and sometimes more effort on how to make use of them. So long as they are competent, as well, this passion means they are bringing real skills to the team that they will not only know but share with the team (Chandran, 2008). This passion leads into a passion to learn often meaning the earning of new, and meaningful, certifications.

Testing Hardware

One of the final pieces necessary to conduct a penetration test is to choose your hardware platform. The choice is between that of a desktop machine and a laptop; both of which have their place in penetration testing. Desktops are much larger in size than laptops but offer substantially greater processing power for their cost. Laptops are incredibly mobile and adaptable as some laptops are able to easily swap hard drives, networking cards, batteries etc (Klevinsky et al, 2002).

Desktop computers would be difficult to bring in to perform an internal penetration test due to their size. As desktops are more powerful and do not need to be moved these characteristics would make them a good choice when conducting an external penetration test. Laptops would make the best choice for testing an internal network as they are highly mobile making them easy to take on site or even test separate segments of the network.

One of the most important pieces of hardware for the computers is the networking card because without it there would be no way to communicate with other computers on the network. The card being used needs to have a "promiscuous" mode, that is to say, it needs to be able to "sniff network traffic and obtain user IDs and passwords" (Klevinsky et al, 2002).

Conducting a Penetration Test

Defining the Scope

Before a penetration test can even begin there are a few matters that must be handled. The first of such issues is to sit down with the client and to define the scope of the project. The client will list their goals and expectations of the penetration test which

will help to determine the manner in which the test will be conducted. This will help alleviate many problems throughout the penetration testing process.

The scope of the penetration test is determined by goals and expectations desired by the client. The test can range from small to extensive in nature. It simply depends on what the client wants or needs. A smaller scoped project may consist of only testing the security specific servers and systems requested; or it might just consist of an external penetration test against the web servers. The goal of a smaller scope test is to find the weaknesses and vulnerabilities in specific areas in an organization.

An in-depth penetration test however would be to "attack" the organization from all sides trying to find ways to bring it down (without doing so). This "attack" is done through the use of external and internal testing, as well as social engineering. An in-depth test takes a great deal more time to perform and requires a wider range of resources to be completed. An in-depth test however will give an organization are far better view of their overall security, how the security of one system affects another, and how to improve it.

The scope of the test changes the resources necessary to bring the test to a successful completion. An in-depth test often requires a greater range of tools to be used as the purpose is to attack the network from all angles. It will also require a team that has both the knowledge and experience necessary to detect and exploit the extensive range of possible network vulnerabilities. Smaller scoped projects will naturally require a more refined set of tools to complete a specific task. As OSS tools have their source code available it allows for teams to modify or refine tools to specific

tasks (Tayal, 2009). In some instances the development of a completely new tool may need to be done.

One of the biggest concerns that can be resolved by having the client write down their expectations is defining the legal aspects of the project. Liability is a major concern, especially if something goes wrong, and negotiating that rocky path now protects both the client and the testing body in the long run. At this time, it is appropriate to request network documentation to facilitate in both the assigning of personnel and optimally conducting the penetration test.

Assigning Resources

By using the goals and expectations defined by the client, assigning personnel should be fairly straightforward; assign personnel based on their applicable skill set. For example, if the scope of the project shows the need for customized tools, assign a coder to the project. However, the scope of the project may at times be beyond the abilities or expertise of the personnel. In instances such as this, contract hiring would be an acceptable solution. Other alternatives include training select personnel prior conducting the penetration test.

When assigning personnel to the project it is important to assign members whose skills either compliment or augment one another. Teamwork in a penetration test is important because various vulnerabilities and exploits require a wider range of knowledge than any one assigned member is likely to possess.

After the team has been created, it is necessary to fully discuss the client's goals and expectations for the penetration test so that they are clearly understood. It is

important to share all documentation received from the client after successful negotiations as this is key to the team's ability to design a plan of attack.

Testing

After the team has defined its best course of action comes the actual penetration test. As previously mentioned penetration testing operated in three major veins. External testing, internal testing, and sometimes social engineering comprise the three methods of conducting a penetration test.

During the testing phase of the operation the team will use their OSS and proprietary purchased software to detect network vulnerabilities. Specific vulnerabilities in firewalls and servers allow the penetration tester to gain access to the internal network. After access to the internal network is achieved it is on to the internal testing portion. The goal of the internal network testing is to detect vulnerabilities and exploits that will allow an outside or limited access user to gain access to materials they are not privileged to access.

Social engineering however can take place before, during, or after external penetration testing. The goal of social engineering is to circumvent in place security measures to gain access to confidential information. It is often used to test for security gaps and to check for compliance to set security standards.

Penetration Report

The report is undoubtedly one of the most important parts to any penetration test. While it may not seem like an actual part of the testing it is the manner in which the results of the testing are reported. The penetration report is proof of a test well done, even if the results were unexpected.

It is understood that the steps taken during the penetration test and their results should be included in the report, but what else should be included? As the results of the penetration test will be shown to the people who authorized it, usually people who are not technical, which means the report will need to be broken down into different sections (SANS 1, 2006). SANS Institute suggests breaking the report down into "an Executive Summary, a Management Summary that includes some high-level operational details such as server IP addresses and what needs to be fixed immediately, and a Technical Summary with very specific results and remediation suggestions" (2006). This will ensure that all that read the report will be able to understand the problems with their computer security and how to improve upon it.

A proper penetration test report does not merely report what vulnerabilities were present on each system. It goes beyond simply reporting the vulnerabilities by demonstrating "how this system was accessed, and then explaining the vulnerability and exploit" (SANS 1, 2006).

> *For example, if a DMZ mail server was compromised, and then used as a "jump point" to access other systems, then this entire attack path should be laid out in detail for everyone to understand. The exploitation of trust relationships is a key factor that is difficult to represent by simple "canned" exploits or attack methods. (SANS 1, 2006)*

Conclusion

Technology is one of the operational foundations to our financial and business sectors, and to our government. Information Technology is a constantly evolving field and, as such, security policies should evolve with them. Being behind is not an option, it

is necessary to be proactive about security. Ethical hacking in today's world is a proactive step in protecting and ensuring the security of the confidential information of businesses and their clients.

Bibliography

Beaver, K. (2004). Hacking for Dummies. In K. Beaver, *Hacking for Dummies* (2nd Edition ed., p. 378). Wiley.

Bradley, T. (2009). *Introduction to Vulnerability Scanning*. Retrieved June 28, 2009, from About.com: Internet / Network Security: http://netsecurity.about.com/cs/hackertools/a/aa030404.htm

Card, O. S. (2002). *Ender's Game*. Starscape.

Chandran, R. (2008, July 24). *What we look for in our Penetration Testers*. Retrieved June 29, 2009, from PLYNT Security Testing Verification and Certification: http://www.plynt.com/blog/2008/07/what-we-look-for-in-our-penetr/

CORE. (2009). *Meeting Compliance Requirements for Security Testing*. Retrieved June 28, 2009, from CORE Security Technologies: http://www.coresecurity.com/content/compliance-requirements

CramSession. (2009). *CISSP (R) Certification Training Resources*. Retrieved June 28, 2009, from CramSession: http://www.cramsession.com/certifications/isc2/cissp.asp

Department of Defense. (2008). *Information Assurance Workforce Improvement Program* (DoD 8570.01-M) http://www.dtic.mil/whs/directives/corres/pdf/857001m.pdf

eHosting Datafort. (2009). *Internal Penetration Testing*. Retrieved June 28, 2009, from EHDF: http://www.ehdf.com/internal-penetration-testing.html

Espenschied, J. (2008, May 27). *Five free pen-testing tools*. Retrieved June 29, 2009, from ComputerWorld Security: http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9087439

Ethical Hacker Network. (2008). *GPEN - GIAC Certified Penetration Tester*. Retrieved June 28, 2009, from The Ethical Hacker Network: http://www.ethicalhacker.net/content/view/180/3/

Freed, A. M. (2009, February 14). *Another Payment Card Processor Hacked*. Retrieved June 28, 2009, from Information Security Resources: http://money.cnn.com/2005/06/17/news/master_card/index.htm

FTC. (2009). *About Identity Theft*. Retrieved June 28, 2009, from Federal Trade Commision: http://www.ftc.gov/bcp/edu/microsites/idtheft/consumers/about-identity-theft.html

Greenburg, A. (2007, November 28). *If Security Is Expensive, Try Getting Hacked*. Retrieved June 27, 2009, from Forbes.com: http://www.forbes.com/2007/11/27/data-privacy-hacking-tech-security-cx_ag_1128databreach.html

Hinders, D. (2009). *What is Computer Hacking?* Retrieved June 26, 2009, from WiseGEEK: http://www.wisegeek.com/what-is-computer-hacking.htm

ISC. (2009). *CISSP Education and Certification*. Retrieved June 28, 2009, from ISC2 Certified Information Security Education: http://www.isc2.org/cissp/default.aspx

ITEDU 490. (2009). *Security Guide Tips.* Muncie, Indiana: Department of Technology: College of Applied Sciences and Technology.

Javelin Strategy and Research. (2007, February). *Identity Theft Surveys and Studies*. Retrieved June 28, 2009, from Privacy Rights: http://www.privacyrights.org/ar/idtheftsurveys.htm#Jav2007

Klevinsky, T., Laliberte, S., & Gupta, A. (2002). *Hack I.T. : Security Through Penetration Testing.* Addison-Wesley Professional.

Koonammavu, B. (2008, December 12). *PCI DSS History.* Retrieved June 28, 2009, from Chief Information Security Officer Network: http://www.ciso.in/pci-dss/pci-dss-history.html

Mehta, P. (2005, April 27). *Guide to penetration testing, Part 3: Penetration testing strategies*. Retrieved June 28, 2009, from SearchNetworking: http://searchnetworking.techtarget.com/generic/0,295582,sid7_gci1083715,00.html

Merriam-Webster. (2009). *Hacking*. Retrieved June 1, 2009, from Merriam-Webster's Dictionary: http://www.merriam-webster.com/dictionary/hacking

Mills, E. (2009, Jan 29). *Global cost of cybercrime hit $1tn, study finds*. Retrieved March 22, 2009, from ZDNet.uk: http://news.zdnet.co.uk/security/0,1000000189,39605987,00.htm

Mullins, M. (2005, July 11). *Choose the best penetration testing method for your company*. Retrieved June 28, 2009, from Tech Republic: http://articles.techrepublic.com.com/5100-10878_11-5755555.html

NIST. (2009, May 8). *Computer Security Division - Computer Security Resource Center*. Retrieved June 28, 2009, from Nation Institute of Standards and Technology: http://csrc.nist.gov/groups/SMA/fisma/overview.html

O'Ferrell, C., & Winkler, I. (2001, August 3). *News and Analysis: Hacking Pros and Cons.* Retrieved June 28, 2009, from Network Computing: http://www.networkcomputing.com/showArticle.jhtml?articleID=8703161&pgno=1&queryText=gbits%5C

Offensive Security. (2009). *Penetration Testing Training and Certification - BackTrack Training*. Retrieved June 28, 2009, from Offensive Security Training: http://www.offensive-security.com/penetration-testing-backtrack-online-training.php

PCI DSS Guru. (2008). *PCI DSS 11.3: Penetration Testing Requirements Clarified.* Retrieved June 28, 2009, from PCI DSS Guru: http://www.pcidssguru.com/pci-dss/pci-dss-113-penetration-testing-requirements-clarified/

PCI Security Standards Council. (2009). *About the PCI Data Security Standard (PCI DSS).* Retrieved June 28, 2009, from PCI Security Standards: https://www.pcisecuritystandards.org/security_standards/pci_dss.shtml

PLYNT. (2006). *Penetration Testing, Applications Security & Security Code Reviews.* Retrieved June 30, 2009, from PLYNT Security Testing Verification and Certification: http://www.plynt.com/resources/learn/penetration-testing/

Priester, C. (2008, June 30). *So You Say You Want a Penetration Test...* Retrieved June 28, 2009, from Prometheus Group: http://www.progllc.com/blogs/37-fed-sec/138-penetration-testing.html

Ricciuti, M. (1996, June 6). *Hacking cost businesses $800 million.* Retrieved June 28, 2009, from CNet.com: http://news.cnet.com/Hacking-cost-businesses-800-million/2100-1023_3-213958.html

Sahadi, J. (2005, July 27). *Breach affects 40M+ credit cards.* Retrieved June 27, 2009, from CNN.com: http://money.cnn.com/2005/06/17/news/master_card/index.htm

SANS 1. (2006, June). Retrieved June 29, 2009, from SANS Institute: http://www.sans.org/reading_room/analysts_program/PenetrationTesting_June06.pdf

SANS. (2009). *DoD 8570.* Retrieved June 28, 2009, from SANS Institute: http://www.sans.org/8570/

Security Monkey. (2006, June 29). *Getting Hired As A Penetration Tester.* Retrieved June 29, 2009, from Toolbox for IT: http://it.toolbox.com/blogs/securitymonkey/get-hired-as-a-penetration-tester-10224

Skoudis, E. (2008, January 15). *SHould social endineering tests be included in penetration testing?* Retrieved June 28, 2009, from SearchSecurity: http://searchsecurity.techtarget.com/expert/KnowledgebaseAnswer/0,289625,sid14_gci1308098,00.html

SOX-Online. (2006). *What is Sarbanes-Oxley.* Retrieved June 28, 2009, from SOX-Online: http://www.sox-online.com/whatis.html

Stern, A. (2008, June 6). *Amazon's Down: It's Hip To Be Down.* Retrieved June 28, 2009, from Center Networks: http://www.centernetworks.com/amazon-down

Tayal, A. (2009, March 24). *Open Source BI: An Alternative to Proprietary Tools.* Retrieved June 28, 2009, from Information Management: http://www.information-management.com/specialreports/2009_133/open_source_bi-10015102-1.html

(Mills, 2009)

(Hinders, 2009)

(Ricciuti, 1996)

(Greenburg, 2007)

(Sahadi, 2005)

(Freed, 2009)

(Beaver, 2004)

(Card, 2002)

(Klevinsky, Laliberte, & Gupta, 2002)

(Mullins, 2005)

(Mehta, 2005)

(Stern, 2008)

(eHosting Datafort, 2009)

(Skoudis, 2008)

(Priester, 2008)

(NIST, 2009)

(CORE, 2009) ($CORE_1$, 2009)

(PCI Security Standards Council, 2009)

(Koonammavu, 2008)

(PCI DSS Guru, 2008)

(SOX-Online, 2006)

(SANS, 2009)

(Ethical Hacker Network, 2008)

(Offensive Security, 2009)

(CramSession, 2009)

(Department of Defense, 2008)

Department of Defense. (2008). *Information Assurance Workforce Improvement Program* (DoD 8570.01-M) http://www.dtic.mil/whs/directives/corres/pdf/857001m.pdf

(ISC, 2009)

(Bradley, 2009)

(Tayal, 2009)

(FTC, 2009)

(Javelin Strategy and Research, 2007)

(SANS 1, 2006)

(O'Ferrell & Winkler, 2001)

(Espenschied, 2008)

(PLYNT, 2006)

(Chandran, 2008)

(Security Monkey, 2006)

(ITEDU 490, 2009)

(Merriam-Webster, 2009)

Bibliography

Beaver, K. (2004). Hacking for Dummies. In K. Beaver, *Hacking for Dummies* (2nd Edition ed., p. 378). Wiley.

Bradley, T. (2009). *Introduction to Vulnerability Scanning*. Retrieved June 28, 2009, from About.com: Internet / Network Security: http://netsecurity.about.com/cs/hackertools/a/aa030404.htm

Card, O. S. (2002). *Ender's Game.* Starscape.

Chandran, R. (2008, July 24). *What we look for in our Penetration Testers*. Retrieved June 29, 2009, from PLYNT Security Testing Verification and Certification: http://www.plynt.com/blog/2008/07/what-we-look-for-in-our-penetr/

CORE. (2009). *Meeting Compliance Requirements for Security Testing*. Retrieved June 28, 2009, from CORE Security Technologies: http://www.coresecurity.com/content/compliance-requirements

CramSession. (2009). *CISSP (R) Certification Training Resources*. Retrieved June 28, 2009, from CramSession: http://www.cramsession.com/certifications/isc2/cissp.asp

eHosting Datafort. (2009). *Internal Penetration Testing*. Retrieved June 28, 2009, from EHDF: http://www.ehdf.com/internal-penetration-testing.html

Espenschied, J. (2008, May 27). *Five free pen-testing tools*. Retrieved June 29, 2009, from ComputerWorld Security: http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9087439

Ethical Hacker Network. (2008). *GPEN - GIAC Certified Penetration Tester*. Retrieved June 28, 2009, from The Ethical Hacker Network: http://www.ethicalhacker.net/content/view/180/3/

Freed, A. M. (2009, February 14). *Another Payment Card Processor Hacked*. Retrieved June 28, 2009, from Information Security Resources: http://money.cnn.com/2005/06/17/news/master_card/index.htm

FTC. (2009). *About Identity Theft*. Retrieved June 28, 2009, from Federal Trade Commision: http://www.ftc.gov/bcp/edu/microsites/idtheft/consumers/about-identity-theft.html

Greenburg, A. (2007, November 28). *If Security Is Expensive, Try Getting Hacked*. Retrieved June 27, 2009, from Forbes.com: http://www.forbes.com/2007/11/27/data-privacy-hacking-tech-security-cx_ag_1128databreach.html

Hinders, D. (2009). *What is Computer Hacking?* Retrieved June 26, 2009, from WiseGEEK: http://www.wisegeek.com/what-is-computer-hacking.htm

ISC. (2009). *CISSP Education and Certification*. Retrieved June 28, 2009, from ISC2 Certified Information Security Education: http://www.isc2.org/cissp/default.aspx

ITEDU 490. (2009). *Security Guide Tips.* Muncie, Indiana: Department of Technology: College of Applied Sciences and Technology.

Javelin Strategy and Research. (2007, February). *Identity Theft Surveys and Studies*. Retrieved June 28, 2009, from Privacy Rights: http://www.privacyrights.org/ar/idtheftsurveys.htm#Jav2007

Klevinsky, T., Laliberte, S., & Gupta, A. (2002). *Hack I.T. : Security Through Penetration Testing.* Addison-Wesley Professional.

Koonammavu, B. (2008, December 12). *PCI DSS History*. Retrieved June 28, 2009, from Chief Information Security Officer Network: http://www.ciso.in/pci-dss/pci-dss-history.html

Mehta, P. (2005, April 27). *Guide to penetration testing, Part 3: Penetration testing strategies*. Retrieved June 28, 2009, from SearchNetworking: http://searchnetworking.techtarget.com/generic/0,295582,sid7_gci1083715,00.html

Merriam-Webster. (2009). *Hacking*. Retrieved June 1, 2009, from Merriam-Webster's Dictionary: http://www.merriam-webster.com/dictionary/hacking

Mills, E. (2009, Jan 29). *Global cost of cybercrime hit $1tn, study finds*. Retrieved March 22, 2009, from ZDNet.uk: http://news.zdnet.co.uk/security/0,1000000189,39605987,00.htm

Mullins, M. (2005, July 11). *Choose the best penetration testing method for your company*. Retrieved June 28, 2009, from Tech Republic: http://articles.techrepublic.com.com/5100-10878_11-5755555.html

NIST. (2009, May 8). *Computer Security Division - Computer Security Resource Center*. Retrieved June 28, 2009, from Nation Institute of Standards and Technology: http://csrc.nist.gov/groups/SMA/fisma/overview.html

O'Ferrell, C., & Winkler, I. (2001, August 3). *News and Analysis: Hacking Pros and Cons.* Retrieved June 28, 2009, from Network Computing: http://www.networkcomputing.com/showArticle.jhtml?articleID=8703161&pgno=1&queryText=gbits%5C

Offensive Security. (2009). *Penetration Testing Training and Certification - BackTrack Training*. Retrieved June 28, 2009, from Offensive Security Training: http://www.offensive-security.com/penetration-testing-backtrack-online-training.php

PCI DSS Guru. (2008). *PCI DSS 11.3: Penetration Testing Requirements Clarified.* Retrieved June 28, 2009, from PCI DSS Guru: http://www.pcidssguru.com/pci-dss/pci-dss-113-penetration-testing-requirements-clarified/

PCI Security Standards Council. (2009). *About the PCI Data Security Standard (PCI DSS)*. Retrieved June 28, 2009, from PCI Security Standards: https://www.pcisecuritystandards.org/security_standards/pci_dss.shtml

PLYNT. (2006). *Penetration Testing, Applications Security & Security Code Reviews*. Retrieved June 30, 2009, from PLYNT Security Testing Verification and Certification: http://www.plynt.com/resources/learn/penetration-testing/

Priester, C. (2008, June 30). *So You Say You Want a Penetration Test...* Retrieved June 28, 2009, from Prometheus Group: http://www.progllc.com/blogs/37-fed-sec/138-penetration-testing.html

Ricciuti, M. (1996, June 6). *Hacking cost businesses $800 million.* Retrieved June 28, 2009, from CNet.com: http://news.cnet.com/Hacking-cost-businesses-800-million/2100-1023_3-213958.html

Sahadi, J. (2005, July 27). *Breach affects 40M+ credit cards*. Retrieved June 27, 2009, from CNN.com: http://money.cnn.com/2005/06/17/news/master_card/index.htm

SANS 1. (2006, June). Retrieved June 29, 2009, from SANS Institute: http://www.sans.org/reading_room/analysts_program/PenetrationTesting_June06.pdf

SANS. (2009). *DoD 8570*. Retrieved June 28, 2009, from SANS Institute: http://www.sans.org/8570/

Security Monkey. (2006, June 29). *Getting Hired As A Penetration Tester.* Retrieved June 29, 2009, from Toolbox for IT: http://it.toolbox.com/blogs/securitymonkey/get-hired-as-a-penetration-tester-10224

Skoudis, E. (2008, January 15). *SHould social endineering tests be included in penetration testing?* Retrieved June 28, 2009, from SearchSecurity: http://searchsecurity.techtarget.com/expert/KnowledgebaseAnswer/0,289625,sid14_gci1308098,00.html

SOX-Online. (2006). *What is Sarbanes-Oxley*. Retrieved June 28, 2009, from SOX-Online: http://www.sox-online.com/whatis.html

Stern, A. (2008, June 6). *Amazon's Down: It's Hip To Be Down*. Retrieved June 28, 2009, from Center Networks: http://www.centernetworks.com/amazon-down

Tayal, A. (2009, March 24). *Open Source BI: An Alternative to Proprietary Tools*. Retrieved June 28, 2009, from Information Management: http://www.information-management.com/specialreports/2009_133/open_source_bi-10015102-1.html